SECTION 2 TABLE OF CONTENTS

11 Oct 2004

Page

SECTION 2 TABLE OF CONTENTS, CONT.

Page

LIST OF FIGURES

Page

2.0 ROLES AND RESPONSIBILITIES

This section lists the organizations and individuals responsible for the execution and day-to-day management of NMCI. This section provides detailed descriptions of their roles and responsibilities in supporting the processes outlined in this guide.

2.1 DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO)

The DON CIO is organized to align and integrate Information Technology/Information Management (IT/IM) programs across the Navy and Marine Corps and to focus department-wide IT/IM efforts on warfighter priorities. Overall leadership responsibility is vested in the CIO, supported by the Deputy DON CIO (Navy) and Deputy DON CIO (Marine Corps). The Deputy DON CIO for Policy and Integration directs the operations of the DON CIO Functional Teams. The teams advance the goals and objectives of the DON IT/IM Strategic Plan.

Figure 2-1 depicts the senior executive staff positions of the DON CIO organization. The Deputy DON CIO (Navy) and Deputy DON CIO (Marine Corps) are responsible for implementing DON IT/IM programs and policies at the service level.

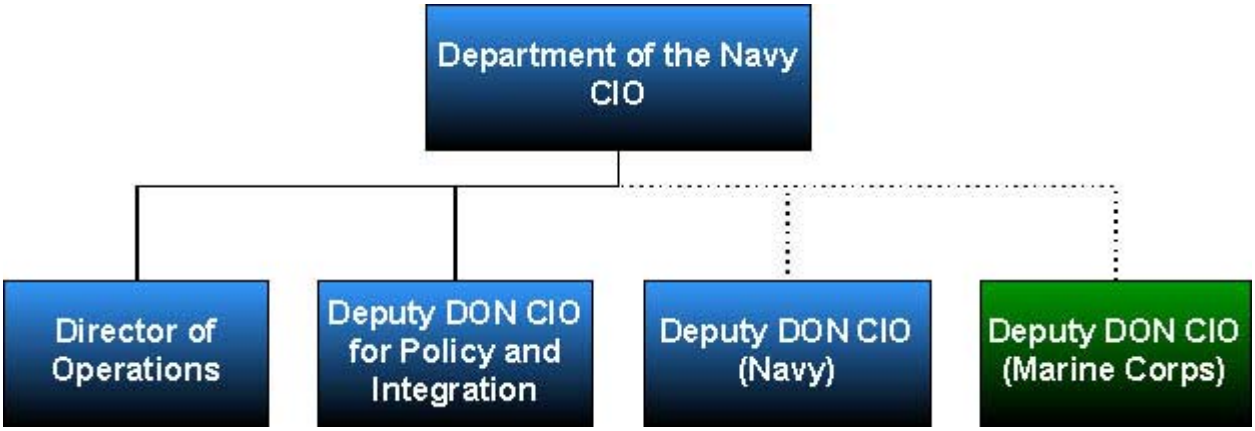

Figure 2-1 DON CIO Organization Chart

2.1.1 Deputy DON CIO (Navy)

The Deputy DON CIO (Navy) is responsible for the following:

- Bring operational IT/IM requirements into alignment with Navy functionality capabilities using developed and established processes and procedures.
- Advise and assist the Chief of Naval Operations (CNO) in achieving network-centric operational capabilities by managing robust global and local networks, employing proven-successful business practices, and integrating IT/IM as it applies to warfighters at sea and the supporting shore establishment.
- Oversee the integration of dispersed sea-based and joint command and control architectures.

- Champion the incorporation of significant industry improvements in IT, in such areas as supply chain and enterprise resource management, into the Navy enterprise.

- Lead the development of strategic plans and implementation strategies for managing global Navy enterprise IT solutions across the Navy.

- Receive requirements from and provide policies and procedures to Commander, Naval Network Warfare Command (NNWC), who is responsible for their implementation.

- Reduce legacy applications and databases in order to support the rapid transition to NMCI.

- Work with and provide guidance to the Functional Area Managers (FAMs), who are ultimately responsible for determining the suite of approved applications and databases used in their business area in order to accomplish the mission.

- Work with Program Executive Office for Information Technology (PEO-IT) to determine the policies and processes for procuring enterprise licenses for applications that have a significant user base across the Navy enterprise, leveraging the capabilities of the NMCI to enhance operations and communications within the Navy.

- Ensure that IT/IM requirements are consistent and compliant with overall Navy/DoD joint architectures and investment decisions.

- Work closely with the DON and the Deputy DON CIO (Marine Corps) to manage "information" and "knowledge" as key strategic resources in order to satisfy Fleet information requirements.

- Oversee the development and implementation of systems, policies, and processes to ensure the integrity, availability, authentication, and safeguarding of Navy information and information display, processing, and storage systems.

- Ensure Navy compliance with evolving national security Information Assurance (IA) policies through the acquisition and implementation of approved IT/IM products.

- Establish, manage, and enforce IT/IM configuration standards for hardware, software, and network connectivity.

- Oversee the development of an enterprise management process for IT/IM configuration control.

- Provide Navy leadership in support of DoD and DON CIO efforts to develop, maintain, implement, and evolve DoD Joint Information Architectures.

- Serve as the Navy lead point of contact (POC) for interaction and coordination with other Service, Joint, DoD, and interagency CIOs for implementing the Global Information Grid (GIG) enterprise solutions.

- Develop, coordinate, and ensure compliance with the Navy IT/IM Plan that serves as a key input to the DON IT/IM Strategic Plan. (The term "information technology" includes "national security systems," as defined in the Clinger-Cohen Act of 1996.)

- Advise the CNO and other senior leadership on all IT/IM-related issues. Key to this function is close coordination and frequent liaison with DON and U.S. Marine Corps CIOs, the Fleet Commanders, Systems Commanders, Commander NNWC, and other Major Claimant CIOs.

- Support DoD and DON CIO efforts to promote effective and efficient design and operation of IM processes throughout the global Navy enterprise.

- Review and critique all Navy IT/IM Support Plans [Command, Control, Communications, Computers, and Intelligence Support Plans (C4ISPs)]. These are prepared and updated at each acquisition milestone in accordance with DoD 5000-series directives, to verify compliance with DoD Joint Technical Architectures and to ensure interoperability, compatibility, and integration with other Joint Warfighting and support systems.

- Oversee the implementation of a Navy-wide IT/IM systems-of-systems testing program to ensure continued interoperability.

- Develop and implement knowledge management strategies that facilitate the improved creation and sharing of knowledge. Knowledge management involves delivering the right information to the right decision-maker at the right time to create the right conditions for new knowledge. It enables more effective and agile decision-making, resulting in greatly improved mission performance.

- Promote results-based performance measures and best practices to improve mission performance and optimize the return on investment for IT/IM.

2.1.2 Deputy DON CIO (Marine Corps)

The Deputy DON CIO (Marine Corps) is responsible for the following:

- Plan, direct, coordinate, and oversee all IT Marine Air Ground Task Force (MAGTF) functions.

- Provide strategic direction to enable the effective and efficient application, moderation, functional integration, acquisition, and management of all IT resources.

- Serve as the senior executive for Marine Corps IT.

- Formulate and publish Marine Corps IT strategy, goals, roadmaps, and objectives.

- Define and issue IT standards and policies consistent with the DoD, DON, and Joint Service mandates.

- Establish the Information Technology Steering Group (ITSG)
- Develop and maintain the Marine Corps Enterprise Information Technology Architecture (EITA)
- Act as the controlling authority for all Marine Corps network and networking activity.
- Act as the Designated Approving Authority (DAA) for the MCEN.
- Evaluate and approve/disapprove the connection of any application to the MCEN.
- Evaluate and confirm compliance of IT pilots and programs to the EITA.
- Prepare policies/orders for processing Marine Corps C4ISPs.
- Confirm that each program has an IA strategy that is compliant with DoD, DON, Marine Corps, and Joint Service policies and standards.
- Serve as IT funding coordinator.
- Develop and manage an integrated Enterprise portfolio of software application ensuring all new development complies with the EITA.

2.1.2.1 NMCI-Specific Functions

The NMCI-specific functions include the following:

- Serve as the Marine Corps sponsor for NMCI.
- Oversee the Functional Program.
- Chair Marine Corps NMCI Transition C2 Operation Cell (CCOC).
- Cochair the NMCI Stakeholders' Council.
- Communicate Marine Corps NMCI policy and requirements.
- Serve as the Marine Corps Decision Authority on NMCI requirements and policy issues.
- Serve as the NMCI subject matter expert (SME) and web content manager in the areas of policy and requirements.

2.1.2.2 NMCI Roles and Responsibilities

The NMCI-specific responsibilities include the following:

- Develop Marine Corps NMCI policy under the guidance/approval of the Marine Corps command, control, communications, computers (C4)/DON CIO.

- Oversee dissemination and implementation of policy for the Marine Corps COI within the NMCI.

- Oversee Marine Corps Network Operations Security Command (MCNOSC) and Computer Network Defense, reporting directly to Headquarters, Marine Corps (HQMC) C4.

- Cochair the NMCI Stakeholders' Council under NMCI Executive Council (Marine Corps, Navy, and DON CIO). (Membership: Major Marine Corps Commands and Navy Activities)

2.1.3 Director NMCI

The Director NMCI manages the acquisition of NMCI under the Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA) and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers within policy constraints.

2.1.4 Functional Area Manager (FAM)

The Under Secretary of the Navy has designated FAMs to reduce IT applications to the minimum number needed to support Navy and Marine Corps requirements. This reduction process standardizes versions to a single application and selects certain applications or suites of applications to perform specific functions across the NMCI Enterprise. It eliminates applications that are not compliant with NMCI standards.

FAMs are responsible for enterprise management of applications and databases assigned within their functional areas (FAs).

NOTE: ***Only applications that have been allowed with restrictions and approved by the FAMs may be deployed in NMCI.***

FAM-disapproved applications will not be loaded onto the technical refresh NMCI seats or be approved for retention on any legacy seat. This includes any application originally FAM approved or allowed with restrictions, but has since been designated FAM disapproved.

For Navy-owned applications that need to be loaded onto a Marine seat, the appropriate Marine FAM should allow the application with restriction (AWR). For Marine-owned applications, the appropriate Navy FAM should do the same. The FAMs from both services should either approve joint mandated applications or designate AWR.

The DON CIO has expanded the functionality of the current Department of the Navy Application Database Management System (DADMS) to support the FAM application rationalization process. Each Command has representatives working closely with the FAM on their applications and databases. Developers and program managers who have questions about the FAM processes should contact their Command FA representative or the FAM Lead.

Key to successful implementation of the FAM process is the participation of the Commands across the functional enterprise.

The operational taxonomy must be accurate to allow informed decisions by the FAMs on portfolio management of applications and systems that support specific operational activity requirements. FAMs are the final approval authorities for operational taxonomies and may modify operational taxonomies for their own FAs only. As stakeholders, FAMs may make change recommendations to other FAMs for consideration and approval.

FAMs are responsible for overall enterprise software management and the execution of specific responsibilities that include, but are not limited to the following:

- Oversee the activities of Functional Data Managers (FDMs).
- Meet process requirements for information gathering and consensus.
- Ensure that the FA has written mission statements, objectives, and a vision in place as a basis for analysis.
- Ensure that the FA has written internal policies in place to guide the FAM Partnership Team on internal FA issues and decisions.
- Cooperate in the identification and funding of required resources to support process execution.
- Cooperate in the identification of initiatives to help ensure that FA enterprise application-and-database management is achieved within the FA and across the enterprise.
- Monitor and approve the progress of the FAM Partnership Team through the major steps in the FAM Mid-Term Application and Database Rationalization Process, as appropriate.
- Control and assign authorities and privileges to Commands that are required to complete and maintain relevant sections of the Integrated Solution Framework (ISF) Tools Database/DADMS data-gathering tool.
- Maintain a relevant and accurate operational taxonomy in ISF Tools Database/DADMS.
- Identify and appoint the Functional Lead and Technical Lead for process execution.

2.1.4.1 FAM Lead

The FAM Lead develops and implements the process execution planning timeline with FAM approval.

2.1.4.2 Functional Lead

The Functional Lead performs the following tasks:

- Communicate formal intent and/or commitment to fully support FAM Mid-Term Application and Database Rationalization Process.

- Provide management oversight for process scheduling, resources, execution, and integration.

- Identify and appoint a FAM Partnership Team, with FAM approval.

2.1.4.3 Technical Lead

The Technical Lead may be a contractor or an in-service Government individual. At the discretion of the FAM, a contractor may be procured to form the basic FAM Partnership Team and to execute the entire process with assistance from designated FA SMEs. FA SMEs may be tasked to support contractor efforts on a full-time or part time basis.

2.1.4.4 FAM Partnership Team

The FAM Partnership Team provides the necessary expertise to execute the full spectrum of FA business and operational requirements analysis and validation for the FAs.

2.1.5 Functional Data Manager (FDM)

The FDM is responsible for implementing functional processes to produce and monitor the use of databases within and across FAs, information systems, and computing and communications infrastructures. FDMs are appointed by the FAMs and are responsible for the following tasks:

- Assist program managers and other system developers in registering system/application (metadata) and data exchange formats and maintaining the metadata baseline.

- Develop and maintain FA views of the DON data architecture.

- Develop candidate DoD standard data elements in coordination with the respective Functional Data Administrator (FDA).

- Coordinate with applicable stakeholders to ensure that DoD-proposed data standards are usable by DON systems.

- Designate the Authoritative Data Source (ADS) for its respective FAs and maintain the designation in the DADMS using processes and procedures approved by the DON CIO.

- Control and assign authorities and privileges required for completing and maintaining the applicable database information in DADMS, under their applicable FAM authority.

2.2 DESIGNATED APPROVAL AUTHORITY (DAA)

2.2.1 Navy NMCI DAA

As the Navy NMCI DAA, NNWC has the responsibility and authority to decide whether to accept the security safeguards prescribed for an Automated Information System (AIS). The DAA is the official authority responsible for issuing an accreditation statement that records the

decision to accept those safeguards. The Navy NMCI DAA is responsible for the following tasks:

- Establish and promulgate the guidelines and security requirements applicable to the NMCI network and the software that operates on that network.
- Ensure the system accreditation for the enterprise.
- Ensure that the AIS security mechanisms enforce the security policy of the enterprise.
- Identify all security-related information required to support the FAM application and database management process.
- Ensure that security and information assurance data entered in the ISF Tools Database/DADMS is correct for each application and database.
- Remove all applications and databases from designated networks that are not included in the FAM portfolio of applications and databases in the ISF Tools Database/DADMS.
- Control and assign roles and responsibilities to designated personnel for completing and maintaining the security and information assurance data in the ISF Tools Database/DADMS.

2.2.2 Marine Corps NMCI DAA

The Marine Corps CIO/Director C4 is the DAA for the Marine Corps. The DAA responsibility has been delegated to the IA branch head. Marine Corps NMCI DAA tasks include the following:

- Evaluate and approve/disapprove the connection of any application to the MCEN.
- Evaluate and approve/disapprove the connection of any application to the Marine Corps NMCI COI.

2.3 COMMANDER NAVAL NETWORK WARFARE COMMAND (NNWC)

NNWC is the Navy central operational authority for space services, network, command and control, IT requirements, and information operations in support of Naval forces afloat and ashore. NNWC is responsible for the following tasks:

- Provide a single source of information support to the Fleet through assumption of central responsibility and authority over all aspects of IM.
- Serve as the advocate for operational forces in the development and fielding of IT, information operations, and space.
- Perform such other functions and tasks, as directed by higher authority.

- Provide approval authority for the deployment of all Navy releases into the NMCI environment.

- Prioritize and schedule releases for submission to EDS.

- Operate a secure and interoperable Naval network that enables effects-based operations and innovation.

- Coordinate and assess the Navy network, command and control, IT, information operations, and space requirements.

- Operate and maintain the Navy global IT systems and services, including enterprise networks, through assigned worldwide communications activities and related contracts that support Warfighting operations and command and control of Naval forces.

- Serve as the single focal point for Navy base-level communications policy, procedures, and resources, and operation and management of the Navy Base Level Information Infrastructure (BLII).

- Operate "Information Technology for the 21st Century" (IT-21) program to upgrade shipboard networks.

- Oversee the Navy computer network attack and defense work through IT-21 and the NMCI procurement with EDS.

2.4 MARINE CORPS NETWORK OPERATIONS SECURITY COMMAND (MCNOSC)

The MCNOSC provides global network operations and computer network defense of the MCEN in order to facilitate seamless information exchange in support of Marine and Joint Forces operating worldwide. The MCNOSC concurrently provides technical leadership for service-wide initiatives that utilize the enterprise capabilities delivered by the MCEN.

The MCNOSC exploits networking expertise and technologies to expand and enhance services to the war fighter so that the network is developed as a weapon to achieve decision superiority. The MCNOSC is responsible for the following:

- Control day-to-day NMCI network operations and C2 Operation Cell (CCOC) within the Marine Corps COI.
- Direct operational execution and contractor interface.
- Coordinate enterprise network operations with Director NMCI and Commander NNWC.
- Provide Tactical & Deployed Support /Computer Network Defense (CND).
- Implement policy formulated by HQMC C4.
- Act as primary interface with the NMCI contractor for network operational, performance, and technical issues.
- Coordinate with and take direction from US STRATCOM chain of command for the defense of the NMCI.

- Act as primary Marine Corps interface with the DISA Global Operations Support Center (GOSC).
- Monitor and collect real-time data and provide to PM NMCI in support of their contractor performance evaluation efforts.

2.5 NAVY NMCI PROGRAM MANAGEMENT OFFICE (PMO)

2.5.1 Enterprise Application Group for Legacy and Emerging (EAGLE)

The Navy PMO created the EAGLE Team to focus on the following information:

- Critical Joint Applications (CJAs) listed in the NMCI contract

- Developer- or Command-owned applications in order to certify applications once at the enterprise or developer's level rather than retesting and certifying applications at each individual site

- All application related information in order to provide the focal point for the Site Solutions Engineering (SSE) teams.

The EAGLE Team is divided into the following teams:

- Data Management Team (DMT)
- NMCI Software Configuration Management (NSCM)
- Claimant CDA Support (CCS)
- Quarantine Upgrade Emerging Support Team (QUEST)
- NSCM Application Prioritization and Scheduling Team
- QUEST Regional Deployment Team (Q-RDT)

2.5.1.1 Data Management Team (DMT)

The DMT performs the following tasks:

- Maintain the ISF Tools Database as the "data repository" for all applications deployed in NMCI.

- Oversee accuracy and data integrity and maintain consolidated application data in one central and accessible location.

- Provide tool configuration, data cleanup, and maintenance.

- Support all levels of users throughout all steps of the transition process and the developer submission process.

- Reduce the amount of rework required by the developer and by each site team on previously encountered applications.

2.5.1.2 NMCI Software Configuration Management (NSCM)

The NSCM organization supports the NMCI PMO by providing management oversight and tracking of releases submitted for deployment in NMCI. The NSCM organization coordinates its efforts with the EDS Application Program Managers (APMs) to facilitate the test, certification, and deployment of application releases to the NMCI enterprise. The NSCM acts as a liaison between a myriad of NMCI activities and helps to resolve issues.

The NSCM is responsible for the following tasks:

- Process, prioritize, and schedule RTD-sponsored applications.
- Technically review Release Deployment Plans (RDPs) and document the Test, Certification, and Deployment processes.
- Provide metrics reporting and application status to developers, NNWC, EDS, and the NMCI PMO.
- Provide training and education to developers through quarterly NMCI conferences.
- Develop and maintain internal processes for processing, tracking, and reporting status throughout the test and deployment life-cycle.
- Provide direct supervision and management of NSCM internal QUEST and CCS activities.
- Track status of Navy NMCI Interim Authority to Operate (IATO)/Authority to Operate (ATO) through the NNWC DAA approval process for RTD applications.
- Develop, maintain, and disseminate messages on the communication test, certification, and deployment status during the various stages of the RTD process.
- Identify RTD-developed NMCI enterprise solutions for quarantine/kiosk applications to reduce the legacy network and to eliminate dual desktops.

2.5.1.3 Claimant CDA Support (CCS)

The CCS focuses on educating developers on the requirements for the Development, Testing, Certification, and Deployment processes in NMCI enterprise. The CCS performs the following specific tasks:

- Provide guidance in the collection and submission of media.
- Create Central Design Activity Request for Service (CDA RFS) documentation.
- Act as technical liaison with EDS throughout the process.
- Use ISF Tools Database to store and collect application information.
- Engage developers for legacy and enterprise application solutions.
- Provide metrics and reporting status to NMCI PMO, NNWC, and developers.

- Assist developers with the ISF Tools Database.

2.5.1.4 Quarantine Upgrade Emerging Support Team (QUEST)

The QUEST organization was created to facilitate and support an integrated approach to quarantine/kiosk application solutions, upgraded applications, and new (emerging) applications to transitioned organizations within the NMCI Enterprise. QUEST supports the deployment of upgraded and new (emerging) applications as they move through the RTD process. QUEST works closely with the NSCM CCS to ensure that the required deployment/implementation documentation is submitted on time and in sufficient detail to support deployment. QUEST provides training and coordination to NMCI Activities, e.g., Legacy Application Point of Contact/ Contract Technical Representative (LAPOC/CTR), EDS, NMCI PMO personnel, etc.

The QUEST organization consists of the following personnel:

- QUEST Coordinator
- QUEST Deployment Analyst
- ECCB/Network Operations Center (NOC)/Test Coordinators
- NNWC – EDS Liaisons
- Application Coordinators
- Field Representatives
- Communications Coordinator

QUEST Coordinator

The QUEST Coordinator can be contacted at NMCI_SCM@spawar.navy.mil and performs the following tasks:

- Coordinate all assets to support the deployment of applications to NMCI users.

- Conduct weekly teleconferences with the QUEST field representatives and the EDS APM lead regarding application deployment issues.

- Provide guidance and instruction to QUEST Network Operations Center (NOC), Service Request Management (Move/Add/Change - MAC), quarantined applications (QAPS), ECCB, unplanned, planned, and critical applications coordinators.

QUEST Deployment Analyst

The QUEST Deployment Analyst performs the following tasks:

- Receive, audit, and perform technical review of required deployment documentation, ensuring an appropriate level of detail for deployment of a RTD application.

- Coordinate with appropriate activities to clarify and correct discrepancies.

- Forward the finalized RDP upon completion of the review to APM to support ECCB and NOC deployment activities.

ECCB/NOC/Test Coordinators

The ECCB/NOC/Test Coordinators perform the following tasks:

- Resolve deployment issues and concerns.
- Request deployment reports.
- Establish close relationships with key personnel.

NNWC – EDS Liaisons

The NNWC – EDS Liaisons perform the following tasks:

- Monitor application progression through the process.
- Update the Plan of Action and Milestones (POA&M).
- Track media submission to the Applications Lab in San Diego, CA.
- Provide application reporting to NNWC, NMCI-PMO, and the NSCM Team.

Application Coordinators

Application Coordinators perform the following tasks:

- Monitor the status of all NNWC-approved unplanned RTD applications, planned, quarantine/kiosk , and critical applications that are submitted for testing, certification, and deployment under the RTD process.

- Interface with scheduling, testing, and deployment activities to identify issues and to provide solutions.

Field Representatives

Field Representatives perform the following tasks:

- Facilitate an integrated approach to upgrade and new (emerging) applications deployment and dual desktop resolution to transitioned organizations within the NMCI enterprise.

- Act as the liaison from the local sites to the NRDDG process.

- Work closely with Contract Technical Representatives (CTRs), Activity Contract Technical Representatives (ACTRs), LAPOCs, CIOs, and Commands to provide information, education, and deployment recommendations in the NMCI post transition environment.

Communications Coordinator

The Communications Coordinator performs the following tasks:

- Send informational email messages to facilitate the transition of quarantine/kiosk and new (emerging) applications.

- Communicate the various stages of the RDP to the developer.

2.5.1.5 QUEST Release and Deployment Analyst (Q-RDA)

The Q-RDA section is collocated within the NSCM facility. QUEST support can be requested through email at NMCI_SCM@spawar.navy.mil. The Q-RDA performs the following tasks:

- Provide training and education to LAPOC and CTR/ACTR personnel on the quarantine/kiosk mitigation, application upgrade, and new (emerging) application RDP.

- Work closely with the EDS APMs to ensure that the RDP information is relevant to the Deployment process.

- Engage the EDS APM and Service Request Support (SRS) personnel to coordinate critical information requirements during all phases of the application Deployment process.

- Notify the Q-RDT of impending application upgrade/new (emerging) releases and supporting RDPs.

- Facilitate quarantine/kiosk solutions across multiple regions.

- Provide deployment status and data reporting to NNWC and the NMCI PMO.

- Coordinate application quarantine/kiosk migration, application upgrade, and new (emerging) application activities with the following groups:

  – LAPOC, CTR/ACTR (site)
  – EDS Base Operations (Base Ops)
  – NMCI NOC
  – EDS Service Request Management (SRM) (MAC) Desk
  – Information Assurance Tiger Team (IATT) (quarantine/kiosk reduction)
  – EDS APMs
  – NNWC
  – EAGLE Claimant CDA Support (CCS) personnel.

2.5.1.6 NSCM Application Prioritization and Scheduling Team

This team prioritizes and schedules RTD application releases for testing based on priority, requested deployment date, media availability, deployment status, and the availability of test and certification resources.

2.5.1.7 QUEST Regional Deployment Team (Q-RDT)

The five Q-RDT field activities are located in the Southwest, Northwest, Hawaii, Southeast, and Northeast NMCI regions. The Q-RDT performs the following tasks:

- Provide onsite support to NMCI site personnel.
- Provide appropriate NMCI PMO regional oversight for the NMCI Application Deployment and Migration process.
- Coordinate with LAPOC, CTR/ACTR, EDS Base Ops, and NMCI Help Desk personnel to support required Test/Pilot Deployment and Notification Plans.
- Train site personnel on the RDP.
- Review existing quarantine plans and application to seat documentation in support of deployment planning.
- Coordinate application quarantine migration, application upgrade, and emerging (new) application activities with the following groups:
  - LAPOC, CTR/ACTR (site)
  - EDS Base Ops
  - IATT (quarantine reduction)
  - EDS APMs
  - NNWC
  - EAGLE CCS Activity

2.6 MARINE CORPS NMCI PMO

2.6.1 Marine Corps Systems Command – Information Systems and Infrastructure (MCSC ISI)

The MCSC ISI provides strategic leadership to ensure the timely delivery and sustainment of interoperable, integrated, and quality information technology (systems and infrastructure) and to position the Product Group (PG) to meet the future needs of the Marine Corps.

2.6.2 Program Manager NMCI Inspection/Test Instruction (ITI)

2.6.2.1 Program Manager NMCI ITI

The Program Manager NMCI ITI performs the following tasks:

- Serve as the single authoritative source for all Marine Corps NMCI-related information.
- Provide communications guidance and program-level feedback.

- Provide information updates through Monthly NMCI Naval message SITREPS as appropriate.

2.6.2.2 PM NMCI/ITI Staff

The Program PM NMCI/ITI staff performs the following tasks:

- Serve as NMCI SMEs and web site content managers in all areas of program management and execution.

- Participate in NMCI Working Groups/integrated product teams (IPTs), as appropriate within their FAs of expertise.

2.6.3 Program Manager Enterprise Business Systems Support (EBSS)

The PM EBSS provides effective software lifecycle management for Marine Corps enterprise business information systems in a timely, accurate, and cost-efficient manner, enabling functional area managers to support the Marine Warfighter's mission. EBSS supports the Marine Corps NMCI PMO by providing management oversight, tracking, and Precertification of application releases and facilitates the deployment of applications into the NMCI environment.

To facilitate start-to-finish NMCI application certification and deployment for the Marine Corps, EBSS performs the following tasks:

- Serve as the single POC to support deployment of applications for the Marine Corps into the NMCI environment.

- Advise and assist Marine Corps FAMs/application sponsors and developers throughout the NRDP.

- Ensure Marine Corps process integration with the NRDDG.

- Coordinate application release efforts with the Marine Corps Application Sponsors and EDS Application Project Managers (APMs) to track and monitor the status of application releases, provide liaison between the Marine Corps Application Sponsor and APM, assist in the resolution of problem areas, and coordinate deployment activities.

- Serve as liaison for Director, NMCI, EDS Applications Test Lab, HQMC C4, MCNOSC, PM NMCI and Joint PMs.

- Manage and maintain Marine Corps Applications and Integration Testing (MCAIT) Lab to support existing and new (emerging) applications.

- Provide Precertification of applications for NMCI Functional and IA Compliance.

- Provide Advance Publisher .msi packages for submission to EDS Applications Test Lab.

- Assist in ARDRA/Pilot Test and deployment process.

- Serve as the Marine Corps NMCI Release Scheduling Manager.

- Schedule applications for pre-certification at the MCAIT Lab in accordance with prioritization set by HQMC (C4), and coordinate prioritization and scheduling for final certification and deployment at EDS Applications Test Lab.

- Integrate and maintain MCASE database for tracking Requests to

- Deploy (RTD)

- Interface MCASE information with ISF Tools Database and DADMS.

- Serve as the Marine Corps NMCI Software Configuration Manager.

- Ensure enterprise level configuration management of applications and minimize scheduling delays in deployment through the implementation of change and configuration management policies, procedures, and processes in compliance with NRDDG.

- Serve as the web site content manager for USMC NMCI application processes.

2.7 COMMAND RESPONSIBILITIES

This section addresses roles and responsibilities of a Command. A Command is defined as a Navy claimant or Echelon II or Marine Corps Forces Command (i.e., MARFORPAC, MARFORLANT, and MARFORRES).

2.7.1 Sponsoring Command

- Report to CNO or higher as a normal part of operations.
- Exercise application management over all subordinate units or organizations.
- Supported by the Program of Record-Program Manager (POR-PM) and developer.
- Provide program and content oversight of the applications and releases.
- Play a review and approval role in the RTD.

2.7.2 Program of Record Program Manager ((POR-PM)

The Program of Record (POR) is a formally funded program or system in support of Navy and Marine Corps requirements. The Program Manager (PM) for a POR is an office or individual who has program responsibilities for an application. These responsibilities include, but are not limited to, funding and maintaining the application. The POR-PM tasks include the following:

- Conduct periodic reviews of their applications to determine if they are current or require a more detailed review and update.

- In conjunction with the developers and FAMs, develop a strategy to retire obsolete applications.

- Ask the Command CTR to update the rationalized list in the ISF Tools Database/RFS.

  NOTE: Application mapping in NET can only occur if the application currently resides on the rationalized list in the ISF Tools Database for the ordering Command.

2.7.3 Developer

A developer is a vendor, organization, or segment of an organization within a DoD component that develops, modifies, maintains, tests, documents, and deploys significant IT/National Security System (NSS) software and its associated support functions and activities substantially in-house. Excluded are organizations that primarily serve in the inherently Governmental role related to the acquisition and management oversight of software systems, e.g., Program Executive Offices (PEOs), PMs, and Special Project Offices (SPOs).

Significant IT/NSS software is defined as software that meets one or more of the following criteria:

- In use Major Command-wide, Component-wide, at multiple installations, or in a broader scope.
- Support DoD/Component business processes.
- Constitute mission critical/essential system(s).
- Consist of multiple nonmission critical/essential applications.

Associated support functions and activities relate to software development such as requirements, design, code, test, documentation, CM, replication/distribution, training, operations, development environment support, field support, and user assistance.

For the purposes of this guide, a developer is any organization, site, group, department, division, unit, section, or individual or Government-sponsored contractor or vendor, who wants to introduce a new (emerging) application or change to an existing application within NMCI environment.

Developers are responsible for ensuring that their releases are compliant with Navy information assurance, boundary, and GPO policies prior to deployment within NMCI. Developers are responsible for adhering to the requirements for developing and migrating applications that comply with TFW, NMCI, IT-21, Outside-Continental United States (OCONUS) BLII architectures, and DON standards.

2.8 ELECTRONIC DATA SYSTEMS (EDS)

EDS provides strategy, implementation, business transformation, and operational solutions for digital enterprises. EDS is the prime contractor supporting NMCI.

2.8.1 Applications Lab

Developers are responsible for providing an Application Submission Packet to the Applications Lab in accordance with Section 6.0. The Applications Lab has both an unclassified application testing facility and a separate classified application testing facility.

Upon receipt of the Application Submission Packet, the Applications Lab is responsible for completing the processes contained in Section 6.0 that support the introduction of new (emerging) applications and updates, upgrades, patches, fixes, and quarantine/kiosk solutions for existing applications.

2.8.2 Site Manager (SM)

The SM, also referred to as Base Operations Manager (BOM), is the lead representative of EDS at each site. The SM is responsible for the delivery of all NMCI services at the designated location. The SM has the following service-delivery roles:

- Support "as-is" applications during the Assumption of Responsibility (AOR) period.

  NOTE: AOR is the date when responsibility for operating the “as-is” environment and for work defined by the ordered NMCI CLINs shifts from the Government and its local contractors to the ISF.

- Support migration/transition during the cutover period.
- Support post transition daily production of existing and new Navy requirements.
- Coordinate EDS operations for the site.

2.8.3 Application Project Manager (APM)

An EDS APM is assigned to each new (emerging) application or application change that enters the Deployment process. The APM is responsible for moving the application through the process and coordinating all tasks and teams required to meet this goal. The APM performs the following tasks:

- Notify the Navy PMO and developer of the assignment to manage the application deployment project.

- Act as the single POC for all status information of an application in the Deployment process for the PMO and the developer.

- Manage the application throughout the Deployment process and coordinate the required work by different EDS teams to accomplish the NMCI Certification and Deployment.

- Update application project information in Project InVision (PIV) to correct the weekly dashboard status.

- Create and submit the Request for Change (RFC) form and collect materials for the submission package for ECCB.

- Coordinate the ECCB presentation and invite the developer and PMO representatives to support the presentation (as needed).

2.9 ENTERPRISE CHANGE CONTROL BOARD (ECCB)

The ECCB is composed of IA and operations personnel from EDS, the Navy, the Marine Corps, and the PMO. Section 6.0 provides more detailed explanation of the ECCB process. Tasks include the following:

- Assess the overall risk exposure.
- Examine whether the application is needed in the enterprise.
- Review all submitted documentation.
- Approve releases that meet all ECCB requirements to continue in the deployment process. .